**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF NEW YORK**

TALENTHUB WORLDWIDE, INC.,

Plaintiff,

- against -

TALENTHUB WORKFORCE, INC.; ERIC GOLDSTEIN; STANDARD CONSULTING, INC.; DIANE POREMBSKI; PATRICIA KAMPEL; TANYA WILSON (WELLARD); JEANNINE TRIOLO; VALERIE WEST; JOSEPH LIPINSKI; and J COMPUTER PRO, INC.

Defendants.

Case No.24-civ-6264 (LGS)

**PLAINTIFF'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS**

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

**Page(s)**

**Cases**

**Statutes**



**Other Authorities**

Plaintiff Talenthub Worldwide Inc. ("Plaintiff" or "Worldwide") submits this Memorandum of Law in opposition to Defendants' Motion to Dismiss the First Amended Complaint.

## PRELIMINARY STATEMENT

Defendants engaged in the wholesale theft of an entire business operation of a temporary staffing business operated by Plaintiff Worldwide. Among the property taken were its computers, a computer server, and access to its cloud-based software platform from which the business was operated and which contained a massive trove of data, including valuable confidential and proprietary information, and trade secrets. Defendants stonewalled about much of this theft for approximately 21 months, lied to cover up the theft of physical computers and fraudulently concealed such conduct with more false statements.

The First Amended Complaint ("FAC"), ECF No. 41, contains twelve counts including two counts related to the Defend Trade Secrets Act (18 U.S.C. § 1836) ("DTSA") and one related to the Computer Fraud and Abuse Act (18 U.S.C. § 1030) ("CFAA") and 10 other counts alleging various state law claims including misappropriation of confidential information, unfair competition, breach of fiduciary duty, unjust enrichment, conversion and tortious interference with contractual business relations.

Defendants, in their Memorandum in Support of Defendants' Motion to Dismiss Plaintiff's First Amended Complaint ("MTD"), ECF No. 48, seek to dismiss the first three counts of the FAC with prejudice, and argues, further, that the Court lacks subject matter jurisdiction to hear the case.

Defendants' arguments should be rejected. The Plaintiff's Computer Fraud and Abuse Act claim was properly filed within two years of the discovery of the damage to the computers that are the subject of the count. Even if the Court found that the statute of limitations started at some

earlier date, that time was clearly tolled by Defendants' misconduct. Defendants wrongfully withheld the subject computers from Plaintiff preventing them from discovering the actual damage to the computers and the unauthorized access of them until September 2023. Defendants wrongful taking, withholding, unauthorized use, and fraudulent concealment of that misconduct would toll the time in which the statute of limitations would begin to run until September 2023 when the computers were returned to Plaintiff.

And Defendants' motion to dismiss the trade secret theft counts should also be dismissed because Plaintiff sufficiently pleaded that its trade secrets were not voluntarily disclosed, that Plaintiff took reasonable steps to protect its information and that Defendants were not authorized to use Plaintiff's trade secrets.

## FACTUAL BACKGROUND

The First Amended Complaint provides an extensive chronology of the actions taken by Defendants to steal the entire business operations of Worldwide and Plaintiff incorporates the contents of the First Amended Complaint by reference herein.

The following addresses a few of the factual assertion by Defendants in the Motion to Dismiss before addressing the legal claims in which Defendants have significantly mischaracterized facts plead in the First Amended Complaint.

Defendants seek to both acknowledge that Gary Glass suffered a significant mental illness by discussing his institutionalization, they also seem to denigrate it (MTD at 7) (stating "nothing could be further from the truth" about the fact that they stole the company while Gary Glass was suffering a serious psychiatric illness). Defendants suggest they needed to flee the location because they feared for their lives yet some of the slurs and ugly language used by Mr. Glass occurred as early as May 2021 and Gary Glass never appeared at Worldwide's offices where the

Defendants worked. And they apparently never felt threatened enough to call authorities during this 6 month episode. Rather, it appears that Defendant Goldstein, understanding Gary Glass's deterioration beginning in May of 2021, began to take steps along with the other Defendants to leave while stealing most of the proprietary information of Worldwide so they could steal its entire business operations.

Defendants claim they already had "full and unrestricted access" to Worldwide's Trade Secrets (MTD at 8) but that was because they only had access as Worldwide employees and kept such access through illegal means by stealing the physical computers from Worldwide's offices and using Joseph Lipinski's status as administrator of Worldwide's email account and Defendant Goldstein's status as signatory of the Avionté business account, which prevented Worldwide from independently asserting control over its own data. Worldwide did want to exclude Workforce once their larcenous intent became clear but lacked the power to do so because Defendants as Worldwide employees and consultants had become the intermediaries to Worldwide's cloud based data and when they moved to Workforce, Worldwide lost its ability to control that data and cut Defendants away from it. Defendants' bald assertion that Worldwide voluntarily gave permission is like saying a victim of a robber gave permission to an armed robber to take his wallet because the robber said, "you don't mind if I take your wallet do you?" and the victim says yes. So, for example, when Worldwide and Workforce were "negotiating" access to Avionté, Worldwide no longer had control of the account.

Meanwhile, Defendants refused to give back computers or give Plaintiff access to all the books and records of Worldwide that they took with them including the Accounting records on Quickbooks and other electronic accounting and business records. It is inexcusable that

Defendants held onto Worlwide's Server for 21 months, and now the evidence shows that there assertions that they did not access the data inside is false (as will be explained in detail below).

Defendants claim that according to the FAC, that all of the claimed Worldwide Trade Secrets were stored in Avionté but this is simply not the case. The FAC explained that this data was "stored on both Worldwide's own computer server and on its cloud-based software program, Avionté3" FAC ¶ 59(a). Nothing in the FAC states that the data on Avionté is identical to all the data saved on the server. And the FAC states that information about temporary employees is stored both on Avionté and the Server. FAC ¶ 59(b). Again, nothing in the complaint says both the Server and Avionté hold identical copies of all the data. See also FAC ¶¶ 59-61 (Worldwide stored additional proprietary information constituting trade secrets and nothing in the FAC says all of this was stored in Avionté). And Defendants wrongfully suggest that the FAC states that each of the Defendants had full access to Worldwide's Trade Secrets when the FAC states that only Defendants West and Goldstein had full access. FAC ¶ 56 (West … like Goldstein had complete access to Avionté) (emphasis added).

Defendants assert that Workforce was created to serve multiple "clients" as a Minority and Women Owned Business Enterprise ("MWBE") but this is also wildly inaccurate. The FAC is very clear that Workforce was set up to serve a single client, identified as Client #1 in the FAC. FAC ¶¶ 100-101 ("As to Gary Glass's understanding, the only purpose for creating Workforce was to assist Worldwide serving the needs of its client, Client #1").[1]

[1] These are the more significant misrepresentation of the facts presented in the FAC. Others are addressed in the legal argument below where necessary. The failure to contradict each and every factual assertion should not be interpreted as an admission that such assertion is true.

## ARGUMENT

### I. PLAINTIFF'S CFAA CLAIM WAS TIMELY FILED

#### A. Legal Standard

A motion to dismiss based on the statute of limitations may be granted "if there is no factual question as to whether the alleged violations occurred within the statutory period." *Old Republic Ins. Co. v. Hansa World Cargo Serv., Inc.*, 51 F.Supp.2d 457, 468 (S.D.N.Y. 1999) (emphasis added). A court is also bound to accept the factual allegations in the complaint as true, drawing all reasonable inferences in favor of the plaintiff. *Roth v. Jennings*, 489 F.3d 499, 510 (2d Cir. 2007) (citation omitted).

And where a Plaintiff alleges that the statute of limitations should be equitably tolled by fraudulent concealment, at the Rule 12(b)(6) stage, a plaintiff is obligated only to plead fraudulent concealment – but is not required to affirmatively prove it at the pleading stage. *See Hinds County, Miss. v. Wachovia Bank N.A.*, 700 F.Supp.2d. 378 at 400 (S.D.N.Y. 2010) (*citing Nine West Shoes Antitrust Litig.*, 80 F.Supp.2d 181, 192-93 (S.D.N.Y. 2000)). "Resolution of a claim of fraudulent concealment so as to toll the statute of limitations is 'intimately bound up with the facts of the case' and is thus not properly decided on a motion to dismiss." *Id*. (citing *In re Mercedes–Benz Anti–Trust Litig.*, 157 F.Supp.2d 355, 374 (D.N.J. 2001) and *In re Sumitomo Copper Litig.*, 120 F.Supp.2d 328, 346–47 (S.D.N.Y. 2000)).

Under the CFAA, the two-year statute of limitations begins to run "2 years of the date of the act complained of or the date of the **discovery of the damage**." 18 U.S.C. § 1030(g) (emphasis added).

### B. The Proper Standard for Determining When the Statute of Limitations Begins to Run Under the CFAA

The statute of limitations only begins to run for a CFAA claim, as to a particular computer, on the date that a Plaintiff discovers either the "damage" to such computer or "unauthorized access" of such computer. *See Sewell v. Bernardin*, 795 F.3d 337, 339-341 (2015).[2] And that requires facts demonstrating that a Plaintiff discovered "that the integrity of her **computer** had been compromised. *Id.* at 341 (Court finding that discovery of impairment of AOL account (when she was denied access) was different than discovery that the integrity of plaintiff's physical computer and AOL's servers). In *Smartix Int'l Corp. v. MasterCard Int'l LLC,* No. 06-CV-5174 (GBD), 2008 WL 4444554, at *3 (S.D.N.Y. Sept. 30, 2008), *aff'd*, 355 F.App'x 464 (2d Cir. 2009), cited by Defendants, the Court made this crystal clear when it explained: "It is the discovery of **the damage**, as oppose to the discovery of other elements of a claim, that begins the clock running."

### C. The Computer Fraud and Abuse Act Claim Was Timely Filed

The Computer Fraud and Abuse Act claim is not time-barred because, contrary to Defendants' arguments, Plaintiff only actually discovered the damage and unauthorized access to its two computers after September 27, 2023, some 21 months after the computer and server were stolen. Prior to that time, the only facts Plaintiff was in possession of was that the computers were missing and Defendants ignored demands to return then (and apparently exercised no due diligence

[2] At the pre-motion conference on December 11, 2024, there was some confusion regarding the standard for determining when the statute of limitations would begin to run CFAA claims as described *Sewell*. In *Sewell* the Court had to determine when the statute of limitations began to run for both CFAA claims and a claim under the Stored Communication Act ("SCA"), 18 U.S.C. § 2701(a). The two acts have significantly different standards for when the statute of limitations runs. Under the SCA, the statute runs as soon as the plaintiff "first … had a reasonable opportunity to discover" the SCA claim as opposed to the CFAA which requires discovery of actual damage or discovery of evidence of unauthorized access. In *Sewell* for example, the Court found that the statute of limitations began to run at different times for the SCA and CFAA counts in that matter. *Sewell*, 795 F.3d at 341-342. During the pre-motion conference there was some discussion suggesting that the "reasonable opportunity to discovery" standard would apply to the CFAA claim, and we discuss this discrepancy here to be sure the proper standard is applied.

to search for them because Defendants claim they were found in a storage closet adjacent to their small office). Using September 27, 2023, as the correct start date for the statute of limitations, the complaint was filed well within "2 years of the date of the act complained of or the date of the discovery of the damage." 18 U.S.C. § 1030(g).

As the facts of *Sewell* make clear, discovery of damage or unauthorized access of a physical computer requires knowledge that the integrity of the computer itself has been compromised. In *Sewell*, the plaintiff alleged different CFAA claims based on unauthorized access of their personal computer and AOL and Facebook accounts that had been hacked and that resided on servers.[3] *See Gates Corp. v. CRP Indus., Inc.*, No. 16-cv-01145-KLM, 2019 WL 10894029 (D. Colo. Nov. 13, 2019) (Court finding one CFAA claim time barred because plaintiff was knew in fact that one defendant had accessed a computer database but finding "genuine issues of material fact as to when [the plaintiff] knew that [a second defendant] accessed its computer systems.)

To use a hypothetical example, if a person steals a computer but never damages the computer or gains unauthorized access to it by turning it on and accessing the data, no CFAA claim exists. The person who stole it would be guilty of a simple larceny, but not a violation of the CFAA. And certainly the statute of limitations cannot begin to run if no crime occurs. All the Plaintiff knew between January 6, 2022 and September 27, 2023 is that the computers were *missing*.[4] Without physical possession of the computer they had no evidence to assert that the "integrity of the computer had been compromised." *Id.* at 341. To put another way, just knowing that a computer is stolen or missing but without the ability to examine the physical computer does

[3] Defendant's citation to cases like *Sewell* and others that involve CFAA violation related to internet accounts are inapposite. *Sewell* distinguished between those plaintiffs who can discover an intrusion into an internet account like AOL and Facebook simply by their lack of access to the account as compared to a physical computer, which requires a physical inspection of the data on the computer itself to determine if damage or unauthorized access has taken place.
[4] In fact, Plaintiff didn't even know the computers were missing until June of 2022 because Defendant's concealed the fact that they had abandoned Worldwide's office space and moved to a new location, taking the computers. FAC ¶ 135.

not provide a plaintiff "with a reasonable opportunity to discover the full scope of [a defendant's] alleged illegal activity." *Id.* at 340.

Defendants wrongly attempt to portray a July 2022 letter by Plaintiff's then-counsel as evidence that the statute of limitations had begun to run at that time. There is no caselaw that says when a lawyer asserts a hypothetical claim, that the statute of limitations has begun. The computers subject to the CFAA claims[5] in the FAC were at the time in the possession of the Defendants – something they repeatedly lied about. FAC ¶ 139. The letter, which listed a number of different legal theories, merely postulated possible, hypothetical claims. Defendants in their motion omit a very significant disclaimer in the July 11th letter, when counsel stated:

> Obviously, we are not in a position to assert all of the potential claims . . . until we receive and review all of the necessary and requested Worldwide and Workforce Documents as well as the Relevant Other Documents, Certainly, Resolution and Settlement can only occur after my Clients have access to this information, which will likely provide the answers to pertinent if not seminal inquiries.

Exhibit A at 4. Further, prior counsel's July 11th Letter also noted the "outrageous" manner in which Defendants had completely ignored numerous demands for return of Plaintiff's property and access to email accounts. Exhibit A at 6 ("My clients need and are entitled to the requested information."); *see also* Exhibit A at 2 ("Gary and Worldwide renew and expand their requests for return of devices … and electronic data … dating back to the time period no later than June 1, 2021 to current."). And Plaintiff repeated this demand numerous times (FAC ¶ 139) all such demands went totally ignored by Defendants and their counsel until Defendants falsely claimed to have only discovered the Server and Goldstein's Desktop in September 2023.

[5] Defendants have sought to clarify which specific computers are the subject of the CFAA claims. To be clear, the CFAA claim in the First Amended Complaint, refer to the computers identified as "the Server" and "Goldstein's Desktop". FAC ¶ 135. Plaintiff is not asserting a CFAA claim as to the Avionté cloud system or cloud-based email systems. See FAC ¶ 42 (Avionté is Worldwide's cloud-based software system).

This paragraph specifically disclaims that counsel had sufficient information to assert the claims he was identifying in the letter and that the ability to file such claims would depend on access to additional information, some of which was wrongfully possessed by Defendant.

But without the computer, Plaintiff could not allege that the Defendants had "deliberately and without authorization accessed Plaintiff's computers for the purpose of misappropriating its trade secrets." FAC ¶ 257. Without the computers, the Plaintiff could not allege that "Defendants … intentionally accessed a protected computer without authorization, and as a result of such conduct, caused damage and loss, in violation of 18 U.S.C. §§ 1030(a)(5)(A)-(C)." FAC ¶ 259. And without the computers, Plaintiff could not allege what damages they incurred. FAC ¶ 260. These are all necessary facts that any Plaintiff would need to possess to allege a legally sufficient CFAA claim.

At worst, all the Plaintiff knew was that the computers were missing. But the fact that a computer is missing does not give rise to a CFAA claim – you must have some evidence from which to infer that the computer was accessed or damaged. The theft of the computers was not more than a supposition before they were returned in 2023, as Plaintiff held no actual proof that Defendants had even physically taken the computers – and Defendants, until the computers were returned, willfully refused to respond with <u>any</u> information – they remained silent until September 2023. And without any information or knowledge that the computers were actually used, there would have been no basis for filing a CFAA claim.

The cases cited by Defendants actually support Plaintiff's position. For example, in *Smartix*, the Court held that the statute of limitations began to run when the plaintiff discovered "the damage to its computer equipment," which it had in its possession. 2008 WL 4444554, at *3. There is simply no way Plaintiff could have discovered "the damage to its computer system" as

long as the computers remained in the possession of the Defendants for 21 months until September 2023. Defendants incorrectly assert that knowing the computers were missing is the same as discovering damage to data on a physical computer – but they clearly are not. Thus, the Defendants argument that the statute of limitation began to run by at least July 11, 2022 is completely misplaced. That statute of limitations did not begin to run until at least until September 27, 2023 when Plaintiff was given back the two computers and they could be inspected for damage and any unauthorized access.

**D. Alternatively, Defendants Fraudulent Concealment of the Intrusion and Damage to the Server and Goldstein's Desktop Equitably Tolls the Statute of Limitations**

The First Amended Complaint, despite the Defendants' arguments to the contrary, alleged sufficient facts to establish fraudulent concealment[6] by the Defendants' wrongful taking, and refusal to return, for 21 months of the Server and Goldstein Desktop so that Plaintiff had no way of alleging, let alone prove, at that point, that Defendants had physically taken or unlawfully accessed and damaged the information contained in said devices in violation of the CFAA. In fact, until September 27, 2023, the Defendants had steadfastly denied that they even possessed Worldwide's computers. FAC ¶¶ 137-39. And without the computers, there was no evidence from which the Plaintiff could have filed a CFAA complaint because they did not possess information sufficient to have alleged any of the statutory elements of the CFAA, particularly any damage to the computers.

[6] Defendants assert that fraudulent concealment is not a theory applicable to CFAA claims simply because the case Plaintiff cited *S.E.C. v. Wyly*, 788 F.Supp.2d 92 at 104 (S.D.N.Y. 2011) (doctrine of fraudulent concealment explained), was a securities fraud case. Defendants offer no caselaw or other analysis as to why the doctrine is so limited to Securities Fraud. In fact, Courts have analyzed fraudulent concealment in CFAA cases. *See, e.g., Gates Corp.*, 2019 WL 10894029 at *16.

Had the Defendants returned the computers within a day or two of, at least, the first demand to return the computers in July 2022, Plaintiff could have hired the forensic computer experts to discover the evidence that the computers had been accessed without authorization and the damage that they caused that is outlined in the Complaint. FAC ¶¶ 144-145.

Thus, Defendants wrongful conduct specifically prevented them from asserting a timely claim, the Defendants knew the relevant facts (that the computers were in their possession and had been accessed and damaged), that their false statements that they accessed the data was intended to prevent them from being accused of CFAA claims, the Plaintiff, without the computers could not, therefore, assert the CFAA claims, and the Plaintiff was forced to rely on such claims for over 21 months because the Defendants were in possession of the Server and Goldstein's Desktop.

And Defendants are wrong when they claim that Plaintiff did not specifically plead facts that make entitlement to estoppel "plausible (not merely possible). MTD at 17. To the contrary, the FAC lays out at length the lies that the Defendants' told about using the computer and the preliminary forensic data that establishes that their claims of not using or accessing the data was false. Defendant simply ignores or omits all of this information in his memorandum as if ignoring it means it doesn't exist.

The First Amended Complaint explained that:

1) "And after being returned by Defendants, a review of the Server … established that data on a Worldwide computer had been accessed and altered or destroyed without Worldwide's permission. Further, this discovery put the lie to Workforce's claim that 'at the time these devices were discovered, the equipment had not been operated on for nearly two years, since January of 2022.'" FAC ¶ 145
2) "There is, instead, substantial evidence that Goldstein and/or other of the Defendants

repeatedly accessed the Server and the computers linked to the server after January of 2022. That evidence includes, but is not limited to, the following information discovered by Plaintiff's examination of the computer equipment returned to Plaintiff." FAC ¶ 146

3) Evidence that the Server was accessed on May 23, 2022, which directly contradicts Defendants' claims that they never accessed the Server. FAC ¶ 147.

4) Evidence on the Server that new "shortcuts" were put on the server on 8/5/22, which directly contradicts Defendants' claims that they never accessed the Server. FAC ¶ 148.

5) The discovery of hundreds of documents on the server's hard drive that are all dated after January 6, 2022 when Defendants' took the Server without permission. FAC ¶ 148. This also shows Defendants were lying when they claimed they did not use the Server when it was in their exclusive control and possession after January 6, 2022 and that the substance of the document show that they are Workforce business records.

Defendants cannot explain how Plaintiff fails to allege fraud if the First Amended Complaint demonstrates time and time again, that the Defendants made false statements based on evidence cited in the complaint. When Plaintiff asks for the computers repeatedly, Defendants ignore those demands for 21 months, and then returned the computers with a false assertion that they just discovered them and never used them. And the First Amended Complaint demonstrates, with specific forensic computer evidence, that such claims are patently false. Such is sufficient to support a claim of fraudulent concealment because it is a reasonable inference from all these facts that the Defendants were willfully withholding the Server and Goldstein's Desktop from Plaintiff for 21 months. And the Plaintiff alleged that all this conduct was done in furtherance of its illegal

and fraudulent scheme to steal the entire business operations of Worldwide. FAC ¶ 4 ("Goldstein and other Defendants moved computers, servers and their entire business operations from Worldwide's business office in Manhattan to another location in Manhattan and began serving Worldwide's clients through Workforce. In the following months, Plaintiff's owners began to learn at least some of what the Defendants had done to them.).

And if the 21 months that the Defendants wrongfully withheld the computers was tolled, the complaint was filed well within the statute of limitations.

It would turn the law on its head to interpret the statute of limitations as a tool used to reward the theft of the only evidence needed to file a claim – the computers that were accessed without authorization and also damaged by the Defendants. The FAC provides a compelling outline of Defendants' intentional misconduct. FAC ¶¶ 133-67 (Full chronological history of the theft and proof of false statements regarding possession and use of Worldwide's computers).

Finally, Plaintiff is filing, contemporaneously with the Court a motion to seek leave to pierce the attorney-client privilege based upon probable cause to believe that the Defendants caused false statements to be made by their unwitting counsel that furthered the crimes and fraud they committed as alleged in the FAC. As the statute of limitations is an affirmative defense, and to the extent that the facts are in dispute about the wrongful taking and use of the subject computers, if the Court is not comfortable denying Defendants' motion to dismiss on statute of limitations grounds at this point, the Court should at least defer any decision on this point until after all discovery has been taken given that Plaintiff is obligated only to plead fraudulent concealment – but not required to affirmatively prove it at the pleading stage. *See Hinds County,* 700 F.Supp.2d. at 400.

## II. PLAINTIFF'S DTSA CLAIMS SHOULD NOT BE DISMISSED

Plaintiff has sufficiently pleaded that the information at issue constitutes trade secrets under the DTSA, including not only customer identities and preferences, but also proprietary business information such as pricing strategies, client lists, and employee data. The First Amended Complaint ("FAC") also adequately alleges that Plaintiff took reasonable measures to protect these trade secrets, including securing access to sensitive information through restricted login credentials and maintaining it on secure company servers, and that Defendants unlawfully accessed and misappropriated this protected information.

### A. The Information at Issue is Properly Pleaded as a Trade Secret

The DTSA defines trade secrets to include all forms and types of business information where (1) the owner thereof has taken reasonable measures to keep such information secret and (2) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information. 18 U.S.C. § 1839(3). Contrary to what Defendants suggest, the information identified as trade secrets in the First Amended Complaint is not limited to customer identities and preferences. In fact, the Plaintiff's claims involve a broad array of proprietary and confidential information that was misappropriated. This includes, but is not limited to, Worldwide's business model, client lists, list of temporary employees, pricing strategies, and several other types of proprietary information, FAC ¶¶ 59-62, all of which constitute trade secrets integral to Plaintiff's business. *See, e.g., Iacovacci v. Brevet Holdings, LLC*, 437 F. Supp. 3d 367, 380-81 (S.D.N.Y. 2020) (non-public sourcing information for clients constitute trade secret); *ExpertConnect, L.L.C. v. Fowler*, No 18-cv-4828, 2019 WL 3004161, at *4 (S.D.N.Y. July 10, 2019) (client lists and contract details constitute trade secrets);

*Tesla Wall Sys., LLC v. Related Companies, L.P.*, No. 17-CV-5966 (JSR), 2017 WL 6507110, at *10 (S.D.N.Y. Dec. 18, 2017) (internal pricing information and research constitute trade secrets). As pleaded in the FAC, these forms and types of business information were developed through extensive research by the Plaintiff, FAC ¶ 63. Even the client identities and preferences lists reflect information related to their specific fields, making them not otherwise readily ascertainable and protected under DTSA. They derive independent economic value from not being generally known to others, and are not readily ascertainable through proper means.

Additionally, it is worth noting that Defendants themselves have previously referred to this same type of data as a "trade secret" in New York State court, which supports the contention that Plaintiff's trade secrets are valuable and have been improperly used by Defendant. Exhibit B.

**B. Plaintiff Adequately Plead Reasonable Measures to Protect Its Trade Secrets**

Defendants' argument that Plaintiff has not sufficiently pleaded reasonable measures to protect its trade secrets is equally flawed.

First, Plaintiff's claims are not limited to the information stored on Avionté, as Defendant suggests. MTD at 20. The First Amended Complaint outlines a broader range of trade secrets that were misappropriated, including information stored in the company servers, and sufficiently pleads that many of the Worldwide trade secrets were produced and stored in the Avionté software and/or saved on the Worldwide Server, which was securely located inside its office, FAC ¶ 64.

Accordingly, the DTSA requires a plaintiff to demonstrate that it took reasonable steps to protect its trade secrets, which may include "sharing information with employees only on a need-to-know basis, emphasizing the need to keep the information confidential ... and frequently reminding employees of the need to maintain confidentiality," *Inv. Sci., LLC v. Oath Holdings Inc.*, No. 20 Civ. 8159 (GBD), 2021 WL 3541152, at *3 (S.D.N.Y. Aug. 11, 2021). As pleaded

in the FAC, login credentials for Avionté were restricted within Worldwide and not shared with anyone other than personnel authorized by Worldwide to do so, FAC ¶ 71, and so was access to the servers located inside Worldwide offices. Any and all trade secrets were shared with employees on a need-to-know basis, to the extent that it was necessary for their specific roles, and with the awareness of the need to preserve the confidentiality of this information.

Plaintiff has sufficiently pleaded that it took reasonable measures to protect its trade secrets, including securing access to sensitive information and enforcing confidentiality obligations for its employees.

**C. The Trade Secrets Were Never Voluntarily Disclosed**

Plaintiff has not voluntarily disclosed its trade secrets, and did not undermine their protection under the DTSA.

Defendants cite to cases where the plaintiff in those cases disclosed trade secrets to outside business partners, and thus were denied trade secret protections. MTD at 21. This is not the case here. Defendants are fully aware of the fact that Workforce was never envisioned to be a separate company from Worldwide, but rather was an entity intended to service one specific Worldwide client, and had no authority to service other Worldwide clients, FAC ¶¶ 100-109.

Furthermore, it should be noted that Defendants distort the circumstance around the "sharing" of the secure login credentials for Avionté in the April 26, 2022 letter. Contrary to Defendants' suggestion, and as the context indicates, it is but a part of the good-faith efforts to resolve the situation in a non-litigious manner, and was not a voluntary disclosure of Plaintiff's trade secrets.

Furthermore, as pleaded, the Defendants were, in essence, holding Plaintiff's data hostage despite repeated demands to give Plaintiff its own data back. Defendants' wrongful

withholding of the data is now being mischaracterized by the Defendants as some voluntary sharing of data. In Defendants' moving papers they refer to a letter suggesting they had been granted full and unrestricted access (which they only obtained as Worldwide employees or consultants) but that letter indicates that the intention was to separate the companies so that each company would have separate passwords/accounts. MTD at 2. In fact, by April 26, much of the damage had been done because Defendant had used their access to Worldwide data to move clients and temporary employees to Workforce accounts.

Therefore, Plaintiff has sufficiently pleaded that its trade secrets were not voluntarily disclosed, and thus Defendants' argument to the contrary is without merit. At this stage, the FAC sufficiently pleads that Plaintiff took reasonable steps to protect its information, and that Defendants were not authorized to use Plaintiff's trade secrets.

## III. COMPLAINT NEED NOT BE DISMISSED WITH PREDJUDICE, LEAVE TO AMEND WOULD NOT BE FUTILE

Assuming, *arguendo*, that any counts were denied, Defendants assert that this Court should, without undertaking any additional determination, deny leave to Plaintiff to present a basis for amending the FAC. Such a decision, in this case, would be premature without understanding which Counts, if any, were dismissed and the legal basis for such dismissal.

> Rule 15 of the Federal Rules of Civil Procedure prescribes a liberal standard for granting leave to amend, exhorting courts to "freely grant leave when justice so requires." Fed. R. Civ. P. 15(a)(2). Nonetheless, "it is within the sound discretion of the district court to grant or deny leave to amend." *Kim v. Kimm*, 884 F.3d 98, 105 (2d Cir. 2018) (citation and quotation mark omitted). It is well settled that a court may deny leave to amend if, for example, the amendment would be futile, if the movant acted with undue delay, bad faith, or a dilatory motive, or if granting leave would result in prejudice to the opposing party. *Foman v. Davis*, 371 U.S. 178, 182 (1962).

*Mosa LLC v. Tumi Produce Int'l Corp.*, No. 17-CV-1331, 2018 WL 2192188 (S.D.N.Y. May 14, 2018)

Defendant wrongfully asserts that Plaintiff amended the complaint because of Defendants' initial pre-motion letter, dated October 16, 2024. MTD at 23. Defendants' counsel is simply speculating and ascribing motives without evidence and meanwhile ignores another more obvious reason – the fact that counsel who filed the First Amended Complaint had replaced prior counsel who filed the original complaint.

Specifically, with regard to the Defendants' motion to dismiss Counts I and II alleging violations of the DTSA, it is simply impossible to determine whether an amendment would be possible until this Court decides Defendants' motion to dismiss and reserve the right to file a letter seeking leave to file an amended complaint and providing the basis for the motion in that letter.

With regard to the CFAA claims, we specifically request that if the Court were to grant the motion to dismiss on statute of limitations grounds, that the Court not dismiss said count with prejudice. As already mentioned herein, Plaintiff is filing contemporaneously with this Response a separate letter seeking leave to obtain certain attorney-client communications under the theory that the Defendants have cause communications to be made to a state court judge and counsel that give rise to the crime/fraud exception of the attorney-client privilege. That letter and exhibits contain significant, and material evidence produced to Plaintiff by computer forensic experts after the First Amended Complaint was filed. And both the evidence cited in the letter and that which would be obtained if the motion were granted, would provide further evidence to both refute the notion that the statute of limitations had elapsed, and, demonstrate that the Defendants have engaged in the fraudulent concealment of their violations of the CFAA.

## IV. COURT DOES NOT LACK SUBJECT MATTER JURISDICTION

Defendants make a prospective or conditional motion that only asserts that there would be no subject-matter jurisdiction if all three counts of the First Amended Complaint were dismissed. Since the Court has obviously not taken any action on those counts, the Defendants' claim that there is no subject-matter jurisdiction is only hypothetical at this point. In other words, such motion is not yet ripe, such that the Court should not "entangl[e] itself in abstract disagreements over matters that are premature for review because the injury is merely speculative and may never occur." *Ross v. Bank of Am., N.A. (USA)*, 524 F.3d 217, 226 (2d Cir. 2008) (internal quotes omitted).

## CONCLUSION

For all the reasons stated above, Plaintiff respectfully requests that the Court deny Defendants' Motion to Dismiss Counts I through III of the First Amended Complaint in its entirety.

Dated: New York, New York
February 7, 2025

Respectfully submitted,

/s/ Anthony M. Capozzolo
Anthony M. Capozzolo
SDNY Bar No. AC-8633
LEWIS BAACH KAUFMANN MIDDLEMISS PLLC
10 Grand Central
155 East 44th Street, 25th Floor
New York, New York 10017
Tel: (212) 897-1970; Fax: (212) 826-7146
anthony.capozzolo@lbkmlaw.com

*Counsel for Plaintiff Talenthub Worldwide, Inc.*